Srno	Question	Option A	Option B	Option C	Option D
1	What are the two main types of cryptosystems?	Classical and Modern	Symmetric and Asymmetric	Public and Private	Static and Dynamic
2	In a symmetric key encryption system	Different keys are used for encryption and decryption	The encryption key is public and decryption key is private	The same key is used for both encryption and decryption	No key is required
3	Which of the following is a component of a cryptosystem?	Firewall	Encryption Algorithm	Web Server	Router
4	The Caesar Cipher is a type of:	Transposition Cipher	Public Key Cipher	Substitution Cipher	Hashing Algorithm
5	Vigenère Cipher is a type of:	Monoalphabetic Cipher	Polyalphabetic Cipher	Transposition Cipher	Block Cipher
6	Which cipher rearranges the letters of the plaintext without changing the actual letters?	Caesar Cipher	Transposition Cipher	Monoalphabetic Cipher	Vigenère Cipher
7	DES is an example of:	Public Key Encryption	Stream Cipher	Block Cipher	Hash Function
8	How many keys are used in Triple DES?	1	2 or 3	4	5
9	AES stands for:	Automated Encryption Standard	Advanced Encryption Standard	Applied Encryption Scheme	Advanced Electronic Security
10	A digital signature provides:	Confidentiality	Integrity	Authentication and Integrity	Encryption
11	Which of the following ensures data integrity?	Encryption	Decryption	Hashing	Compression
12	One major drawback of cryptography is:	Reduced data accuracy	Insecure communication	Increased resource consumption	It removes authentication
13	Bitcoin is:	A symmetric key algorithm	A type of hashing function	A digital currency built on blockchain	A digital signature
14	Blockchain stores data in:	Files	Tables	Blocks	Packets
15	A distributed ledger in blockchain means:	Only one party holds the data	A centralized database	Data is stored at multiple nodes	The ledger is printed
16	Which of the following is not an attack on cryptosystems?	Brute-force attack	Ciphertext-only attack	Firewall bypass	Known-plaintext attack
17	Asymmetric encryption is also known as:	Public key encryption	Symmetric encryption	Stream encryption	Substitution encryption
18	The main advantage of asymmetric encryption is:	Speed	Larger key size	No need to share secret keys	Simplicity
19	Monoalphabetic cipher uses:	Different substitution for each letter	A fixed substitution throughout	A numeric transformation	Bitwise operations
20	Which cipher is considered the simplest form of substitution cipher?	Vigenère Cipher	Caesar Cipher	Enigma Cipher	One-Time Pad

Srno	Question	Option A	Option B	Option C	Option D
21	Which traditional cipher is the most vulnerable to frequency analysis?	Vigenère Cipher	Caesar Cipher	Transposition Cipher	Monoalphabetic Cipher
22	Which key size is commonly used in AES?	64-bit	128-bit	512-bit	32-bit
23	Hash functions are primarily used to:	Encrypt messages	Sign digital documents	Generate message digests	Compress data
24	Which one is not a modern symmetric encryption algorithm?	AES	DES	RSA	Triple DES
25	In cryptography, a message digest refers to:	Compressed message	Encrypted file	Hash output	Decrypted data
26	Which cryptographic tool helps verify that data has not been altered?	Digital certificate	Encryption	Digital signature	Steganography
27	A benefit of cryptography in network security is:	Increasing bandwidth	Reducing latency	Ensuring confidentiality and authentication	Slowing down intruders
28	One drawback of strong cryptographic algorithms is:	Their vulnerability to physical attacks	Their dependence on outdated technology	High computational cost	Limited usage in modern systems
29	A hash function in blockchain:	Converts plaintext to ciphertext	Creates a fixed-length output from any input	Encrypts entire blocks	Verifies user identity
30	The immutability of blockchain is due to:	Encrypted backups	Centralized control	Hash chaining between blocks	Secure cloud storage
31	In asymmetric encryption, the public key is used for:	Decryption only	Encryption only	Both encryption and decryption	Generating hash values
32	The security of asymmetric cryptosystems relies on:	Private networks	Secrecy of algorithms	Computational difficulty of mathematical problems	Data compression
33	Which attack uses precomputed hash values to crack passwords?	Brute-force attack	Dictionary attack	Rainbow table attack	Chosen-plaintext attack
34	Which cipher was used by Julius Caesar in ancient times?	Monoalphabetic Cipher	Vigenère Cipher	Caesar Cipher	Transposition Cipher
35	Which cipher technique involves rearranging the order of characters?	Substitution	Transposition	Hybrid	Hashing
36	What makes polyalphabetic ciphers stronger than monoalphabetic ciphers?	Larger keys	Multiple substitution alphabets	Use of XOR operations	Reverse encryption
37	RSA is based on the mathematical difficulty of:	Integer division	Prime factorization	Matrix inversion	Modular addition

Srno	Question	Option A	Option B	Option C	Option D
38	The key length of RSA typically used for secure communications is:	56-bit	128-bit	2048-bit	64-bit
39	Which of the following is not a property of a good hash function?	Deterministic output	Reversibility	Collision resistance	Fixed-length output
40	A collision in a hash function means:	The same input gives different outputs	Two different inputs produce the same hash	The hash function fails to run	The key is exposed
41	Which of the following is an advantage of cryptography?	Eliminates need for passwords	Increases network speed	Provides data confidentiality and integrity	Allows easy key sharing
42	Cryptography does not protect against:	Data tampering	Network sniffing	User impersonation	Physical theft of data
43	Each block in a blockchain contains:	Only transaction data	Timestamp and hash of the previous block	Public key and signature	A single user's data
44	Blockchain uses consensus algorithms to:	Encrypt data	Verify transactions	Store private keys	Decode hash functions
45	Which of the following is a key feature of blockchain technology?	Centralized ledger	Immutable records	Hidden transactions	Open file sharing
46	Which of the following best defines a cryptosystem?	A program used to send messages	A structure that defines encryption, decryption, and key management	A system for digital marketing	A public ledger of transactions
47	In public-key cryptography, the private key is:	Shared with everyone	Only used to encrypt messages	Kept secret and used to decrypt messages	Used to generate hash values
48	Chosen-plaintext attack (CPA) means the attacker can:	Only see the ciphertext	Only see the public key	Choose arbitrary plaintexts to encrypt and observe ciphertexts	Modify the encryption algorithm
49	The weakness of Caesar cipher is due to:	Its use of a private key	Limited number of possible shifts (25)	Complexity of the algorithm	One-time pads
50	What does a substitution cipher do?	Shifts letters based on their position	Rearranges characters	Replaces each character with another	Encrypts using a key pair
51	Which cipher is considered unbreakable if used properly with a random key as long as the message?	Caesar Cipher	Vigenère Cipher	One-Time Pad	Transposition Cipher

Srno	Question	Option A	Option B	Option C	Option D
52	Which modern algorithm is most widely used in securing wireless networks (e.g., WPA2)?	DES	RSA	AES	MD5
53	The output of a hash function is called:	Key	Message digest	Signature	Ciphertext
54	Which algorithm is considered insecure today due to its small key size and vulnerability to brute-force attacks?	AES	SHA-256	DES	RSA-2048
55	Which term describes the ability to detect unauthorized changes to data?	Confidentiality	Authenticity	Integrity	Obfuscation
56	A digital signature is typically created using:	Hashing only	Symmetric encryption	A sender's private key	A recipient's public key
57	One limitation of public key encryption is:	It is not secure	It cannot be used over the internet	It is slower than symmetric encryption	It uses the same key for both parties
58	Which of the following consensus mechanisms is used in Bitcoin?	Proof of Stake (PoS)	Delegated Proof of Stake (DPoS)	Proof of Work (PoW)	Practical Byzantine Fault Tolerance (PBFT)
59	The process of verifying and adding transactions to the blockchain is known as:	Mining	Forking	Hashing	Signing
60	In blockchain, immutability means:	The chain is centralized	Only administrators can modify data	Once written, data cannot be changed	Data is encrypted with private keys
61	Which property ensures that only the intended recipient can read a message?	Integrity	Confidentiality	Availability	Authentication
62	Which cryptographic method uses two keys mathematically linked together?	Caesar Cipher	Stream Cipher	Public Key Cryptography	Hashing
63	What is key management in cryptography concerned with?	Designing cipher algorithms	Creating long passwords	Generating, distributing, and storing cryptographic keys	Encrypting images
64	Which cipher type is most affected by letter frequency analysis?	Caesar Cipher	Vigenère Cipher	Transposition Cipher	One-Time Pad
65	The Vigenère cipher combats letter frequency attacks by:	Using mathematical operations	Shifting letters randomly	Applying multiple Caesar shifts based on a keyword	Scrambling bits
66	A transposition cipher maintains:	The order of letters	The letter frequency	The position of the key	None of the above
67	Which algorithm is commonly used for digital certificates?	AES	DES	RSA	Blowfish

Srno	Question	Option A	Option B	Option C	Option D
68	Which of the following is a secure hash function?	MD4	MD5	SHA-256	SHA-1
69	In a digital signature, the verification is done using:	Sender’s public key	Receiver’s private key	Receiver’s public key	Sender’s private key
70	Cryptography helps prevent:	Email spam	Data loss	Unauthorized access and tampering	Operating system failure
71	Which of the following is not a goal of cryptography?	Confidentiality	Data redundancy	Integrity	Non-repudiation
72	Non-repudiation ensures:	The message cannot be intercepted	The sender cannot deny sending the message	The message cannot be altered	The recipient cannot view the message
73	What does the blockchain term “genesis block” refer to?	The latest block in the chain	A hash function	The first block in the blockchain	A mining algorithm
74	What ensures transparency in blockchain systems?	Hidden records	Public access to the ledger	Password encryption	Restricted consensus
75	Which of the following makes blockchain resistant to tampering?	Centralized servers	Frequent updates	Cryptographic hash linking of blocks	Open-source licensing
76	Which of the following algorithms is not used for encryption?	AES	SHA-256	DES	RSA
77	The effectiveness of brute-force attacks can be reduced by:	Shorter keys	Hashing the ciphertext	Using strong, longer keys	Sending plaintext instead
78	The purpose of salting in password storage is to:	Encrypt the passwords	Slow down attackers by adding randomness	Convert passwords to base64	Make hashing reversible
79	A digital certificate binds:	A user to an IP address	A private key to a hash function	A public key to an identity	A message to a time stamp
80	SSL/TLS protocols use:	Only symmetric encryption	Only hashing	A combination of symmetric and asymmetric encryption	Steganography
81	A strong hash function must be resistant to:	Compression	Random inputs	Collisions	Encryption
82	Message authentication codes (MACs) are used to:	Encrypt the entire message	Ensure message authenticity and integrity	Store private keys	Hash passwords
83	Which algorithm uses block ciphers in rounds and substitution-permutation networks?	DES	RSA	Vigenère Cipher	SHA-1

Srno	Question	Option A	Option B	Option C	Option D
84	How many rounds does AES-128 perform?	8	10	12	16
85	What is the block size of AES?	56 bits	128 bits	64 bits	192 bits
86	The block size of DES is:	128 bits	64 bits	56 bits	32 bits
87	Which attack assumes access to both plaintext and ciphertext?	Ciphertext-only attack	Chosen-plaintext attack	Known-plaintext attack	Side-channel attack
88	The Avalanche Effect in cryptography means:	All keys generate similar ciphertext	Small input change causes major output change	The algorithm is unstable	The encryption causes a crash
89	Which key pair is used in digital signatures?	Private key to sign, public key to verify	Public key to sign, private key to verify	Both private and public for verification	Symmetric keys
90	What is blockchain mining?	Encrypting wallets	Verifying transactions and adding them to the chain	Buying cryptocurrency	Hacking into blockchain networks
91	Which type of encryption is faster in execution?	Asymmetric	Public-key	Symmetric	Digital signature
92	In cryptography, non-repudiation ensures:	The message has not been altered	The sender cannot deny having sent the message	The message remains confidential	The system can be reset
93	Which cryptographic technique is widely used in blockchain for linking blocks?	Vigenère Cipher	Hashing	RSA	AES
94	The SHA-256 algorithm always outputs a hash of:	128 bits	64 bits	256 bits	Variable length
95	The process of making encrypted data readable again is called:	Transposition	Hashing	Decryption	Obfuscation
96	Which of these is true about the Caesar cipher?	It uses random keys	It is a polyalphabetic cipher	It shifts letters by a fixed number	It scrambles letters without substitution
97	The main weakness of DES today is:	Lack of mathematical proof	Too complex for practical use	Small key size (56 bits)	Vulnerable to chosen-plaintext attacks only
98	Triple DES performs how many DES operations?	1	2	3	6
99	Which of the following is a symmetric encryption algorithm?	RSA	SHA-1	AES	DSA
100	Which attack is based on measuring physical information like timing and power usage?	Brute-force attack	Side-channel attack	Known-plaintext attack	Ciphertext-only attack
101	Blockchain is considered decentralized because:	It is managed by a central database	No single entity controls the data	It uses encryption only	It works offline

Srno	Question	Option A	Option B	Option C	Option D
102	A major benefit of public blockchains is:	High speed	Controlled access	Transparency and trust	Private user data
103	What ensures immutability in blockchain?	Centralized data servers	Editing capabilities	Chained hashes of previous blocks	Frequent software updates
104	In asymmetric encryption, what is kept secret?	Public key	Decrypted data	Private key	Ciphertext
105	Which one of the following is not a block cipher?	DES	AES	RSA	Blowfish
106	What is the primary function of a cryptographic hash function?	Encrypt data	Compress data	Generate a fixed-length output from input data	Create a digital certificate
107	Which cryptographic concept ensures data has not been altered in transit?	Confidentiality	Integrity	Availability	Non-repudiation
108	Which of the following uses both substitution and transposition techniques?	Caesar cipher	Stream cipher	AES	One-time pad
109	In asymmetric encryption, the sender uses:	Their own private key	Receiver's public key	Receiver's private key	Hash function
110	Which of these is considered a hashing algorithm?	RSA	SHA-256	AES	ECC
111	The strength of asymmetric encryption lies in:	The use of one secret key	Key length and complexity of mathematical problems	Quick computation	Compression algorithms
112	What is the most common key length used in RSA today for secure communication?	128 bits	256 bits	512 bits	2048 bits
113	What is a cryptographic nonce?	A hash algorithm	A key management protocol	A one-time random number	A public key
114	Which cipher is polyalphabetic in nature?	Caesar Cipher	Monoalphabetic Cipher	Vigenère Cipher	Transposition Cipher
115	Which of the following is a disadvantage of symmetric key encryption?	Too slow	Needs a secure key exchange mechanism	Only used for digital signatures	Keys are public
116	What role do miners play in a blockchain?	Create new private keys	Reverse transactions	Validate and record transactions	Generate digital signatures for users
117	Which is not a feature of blockchain technology?	Decentralization	Transparency	Mutability	Security
118	Which part of a blockchain block contains the hash of the previous block?	Data	Timestamp	Nonce	Block header

Srno	Question	Option A	Option B	Option C	Option D
119	The term 'ledger' in blockchain refers to:	A mining device	A cryptographic algorithm	A record of all transactions	A type of smart contract
120	What is the main purpose of blockchain consensus algorithms?	Encrypt data on the chain	Improve network speed	Ensure agreement on transaction validity	Track wallet addresses
121	Which of the following provides both integrity and authentication?	Encryption	Digital Signatures	Caesar Cipher	Hashing
122	What is a public key used for in digital signatures?	Encrypt the message	Generate a nonce	Verify the signature	Hash the message
123	Which one is a weakness of symmetric encryption?	Uses complex mathematics	Public key is hard to store	Secure key distribution is required	Slower than asymmetric encryption
124	Which of these is a stream cipher?	DES	AES	RC4	RSA
125	The key length of AES-256 is:	128 bits	192 bits	256 bits	512 bits
126	Which attack method tries every possible key?	Dictionary attack	Chosen-ciphertext attack	Brute-force attack	Known-key attack
127	The one-time pad cipher is:	Unbreakable if used correctly	An example of block cipher	Symmetric and deterministic	Obsolete and weak
128	What does HMAC stand for?	Hashed Message with Authentication Control	Hashed Message Authentication Code	Hybrid Message Authentication Cipher	Hidden MAC Address Cipher
129	Which property ensures that two different messages do not have the same hash?	Avalanche effect	Collision resistance	Key expansion	Substitution
130	Which cipher type relies on permutation of plaintext characters?	Caesar cipher	Substitution cipher	Transposition cipher	Vigenère cipher
131	What does a node in a blockchain network do?	Mines coins only	Stores a full or partial copy of the blockchain	Encrypts wallets	Deletes old blocks
132	Which of the following is an example of a private blockchain?	Ethereum	Bitcoin	Ripple	Hyperledger Fabric
133	Which cryptographic concept does blockchain rely on for block linkage?	One-time pads	Stream ciphers	Hash functions	Symmetric encryption
134	Smart contracts are typically deployed on:	Bitcoin	Ethereum	DES networks	TLS layers
135	Which type of consensus algorithm is used by Bitcoin?	Proof of Stake	Proof of Authority	Proof of Work	Practical Byzantine Fault Tolerance

Srno	Question	Option A	Option B	Option C	Option D
136	What is the primary purpose of cryptography in cybersecurity?	Increase network speed	Protect data confidentiality and integrity	Backup systems	Disable malware
137	Which of these ciphers was developed during World War II?	Vigenère Cipher	Enigma	Caesar Cipher	Playfair Cipher
138	The Playfair Cipher encrypts text in:	Single letters	Pairs of letters	Binary format	Triple letters
139	Which of the following is not a symmetric cipher?	Blowfish	AES	RSA	DES
140	A digital signature can provide:	Confidentiality only	Authentication only	Integrity and non-repudiation	Key distribution
141	What is the correct order of digital signature creation?	Sign → Hash → Send	Hash → Sign → Send	Encrypt → Hash → Sign	Send → Sign → Hash
142	Most common output size of the MD5 hash algorithm?	128 bits	256 bits	64 bits	512 bits
143	A known-plaintext attack assumes:	Access to ciphertext only	Control over the encryption key	Both plaintext and ciphertext are known	Access to the decryption algorithm
144	Which algorithm is considered insecure due to collision vulnerabilities?	SHA-256	AES	MD5	RSA
145	Key escrow is a practice of:	Storing encrypted messages permanently	Backing up private keys with a trusted third party	Revoking digital certificates	Generating symmetric keys
146	In blockchain, a 'fork' typically refers to:	A loss of encryption keys	A split in the chain due to consensus disagreement	A broken cryptographic link	A type of hashing algorithm
147	Which blockchain concept prevents double spending?	Hashing	Nonces	Consensus mechanisms	Time-locks
148	Which of the following is true about block size in blockchain?	All blockchains have the same block size	Block size affects transaction speed and capacity	Block size is irrelevant	It is used only in smart contracts
149	In blockchain, a Merkle tree is used to:	Store private keys	Verify large sets of data efficiently	Generate wallet addresses	Synchronize clocks
150	What is a smart contract?	A legal contract stored offline	A blockchain-based algorithm that enforces rules automatically	A type of asymmetric encryption	A password policy for blockchain wallets